Understanding Anti-Virus Software

Cyber Security Tip ST04-005

Spam is a common, and often frustrating, side effect to having an email account. Although you will probably not be able to eliminate it, there are ways to reduce it.

Anti-virus software can identify and block many viruses before they can infect your computer. Once you install anti-virus software, it is important to keep it up to date.

What does anti-virus software do?

Although details may vary between packages, anti-virus software scans files or your computer's memory for certain patterns that may indicate an infection. The patterns it looks for are based on the signatures, or definitions, of known viruses. Virus authors are continually releasing new and updated viruses, so it is important that you have the latest definitions installed on your computer.

Once you have installed an anti-virus package, you should scan your entire computer periodically.

- Automatic scans - Depending what software you choose, you may be able to configure it to automatically scan specific files or directories and prompt you at set intervals to perform complete scans.
- Manual scans - It is also a good idea to manually scan files you receive from an outside source before opening them. This includes:
    - Saving and scanning email attachments or web downloads rather than selecting the option to open them directly from the source.
    - Scanning media, including CDs and DVDs, for viruses before opening any of the files.

What happens if the software finds a virus?

Each package has its own method of response when it locates a virus, and the response may differ according to whether the software locates the virus during an automatic or a manual scan. Sometimes the software will produce a dialog box alerting you that it has found a virus and asking whether you want it to "clean" the file (to remove the virus). In other cases, the software may attempt to remove the virus without asking you first. When you select an anti-virus package, familiarize yourself with its features so you know what to expect.

Which software should you use?

There are many vendors who produce anti-virus software, and deciding which one to choose can be confusing. All anti-virus software performs the same function, so your decision may be driven by recommendations, particular features, availability, or price. See the references section for a link to a list of some anti-virus vendors. Installing any anti-virus software, regardless of which package you choose, increases your level of protection. Be careful, though, of email messages claiming to include anti-virus software. Some recent viruses arrive as an email supposedly from your ISP's

technical support department, containing an attachment that claims to be anti-virus software. However, the attachment itself is in fact a virus, so you could become infected by opening it (see Using Caution with Email Attachments for more information).

How do you get the current virus information?

This process may differ depending what product you choose, so find out what your anti-virus software requires. Many anti-virus packages include an option to automatically receive updated virus definitions. Because new information is added frequently, it is a good idea to take advantage of this option. Resist believing email chain letters that claim that a well-known anti-virus vendor has recently detected the "worst virus in history" that will destroy your computer's hard drive. These emails are usually hoaxes (see Identifying Hoaxes and Urban Legends for more information). You can confirm virus information through your anti-virus vendor or through resources offered by other anti-virus vendors. See the references section for a link to some of these resources.

While installing anti-virus software is one of the easiest and most effective ways to protect your computer, it has its limitations. Because it relies on signatures, anti-virus software can only detect viruses that have signatures installed on your computer, so it is important to keep these signatures up to date. You will still be susceptible to viruses that circulate before the anti-virus vendors add their signatures, so continue to take other safety precautions as well.

References

- CERT Coordination Center Computer Virus Resources - http://www.cert.org/other_sources/viruses.html#VI
- Computer Security Division: Computer Security Resource Center (CSRC) Virus Information - http://csrc.nist.gov/virus/

Both the National Cyber Security Alliance and US-CERT have identified this topic as one of the top tips for home users.

Authors: Mindi McDowell, Allen Householder

Produced 2004 by US-CERT, a government organization.

Note: This tip was previously published and is being re-distributed to increase awareness.

This document can also be found at: http://www.us-cert.gov/cas/tips/ST04-005.html